Scott C. Pitcock (pro se)
[Address and phone number omitted from public filing in accordance with Civil L.R. 5-1(c)(5); contact information on file]
scott_pitcock@hotmail.com

Amicus Curiae
Scott C. Pitcock (Pro Se)

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES, AFL-CIO, et al.,
Plaintiffs
v.
DONALD J. TRUMP, et al.,
Defendants.

Case No. 3:25-cv-03698-SI

AMICUS CURIAE BRIEF OF SCOTT PITCOCK IN SUPPORT OF PLAINTIFFS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Statutes

Regulations & Executive Guidance

Federal Agency Publications

National Institute of Standards and Technology (NIST) Publications

Other

EXECUTIVE SUMMARY

1. Interest

   a. Amicus is a former GS-12 IT Specialist employed with the U.S. Food and Drug Administration (FDA), and was subject to removal under Executive Order 14210.

2. Purpose

   a. This brief provides firsthand documentation and supporting materials from the perspective of an internal systems analyst, detailing procedural and operational lapses observed following the issuance of EO 14210 on February 14, 2025.

3. Key Content

   a. Amicus makes no personal claim for relief; the sole purpose of this submission is to assist the Court in evaluating the implementation and oversight of EO 14210.

   b. Included are records and statements showing continued systems access following termination status changes, raising compliance concerns under the Federal Information Security Modernization Act (FISMA)[1] and Office of Personnel Management (OPM)[2] credential revocation guidelines.

   c. The official termination notice was received after the effective date of the Temporary Restraining Order (TRO), although faster notification methods had previously been used.

   d. The record reflects interruptions in the interactive process for affected employees.

4. Consideration Requested

   a. Amicus respectfully requests that the Court take this factual record into account when assessing agency compliance with the TRO and other obligations arising from EO 14210.

INTEREST OF AMICUS

Amicus previously served as a GS-12 IT Specialist in the FDA's Office of Digital Transformation and supported the same team as a contractor for several years prior to federal appointment. To provide relevant context for the observations in this brief, amicus offers the following first-person account:

In that role, I managed secure system access across FDA environments, responded to major IT disruptions, and helped enforce cybersecurity protocols under the Federal Information Security Modernization Act of 2014 (FISMA)[1] and NIST Special Publication 800-53[3]. This work included user offboarding, access remediation, and coordination with cybersecurity teams on threat response and evaluating risk. These responsibilities were supported by academic training, including a B.S. in Computer Science and ongoing graduate study in artificial intelligence and machine learning, with a focus on cybersecurity. I was formally recognized for disaster recovery efforts during my service.

These facts are presented solely to establish the operational expertise underlying the technical and procedural concerns that follow.

SUMMARY OF ARGUMENT

Amicus draws on firsthand experience as a former federal IT specialist to document procedural and technical deviations including access control lapses, interactive process gaps, and delayed communication of employment status. These deviations support the plaintiffs' claims concerning due process and agency compliance. In amicus's view, these breakdowns warrant continued judicial scrutiny to ensure compliance and operational accountability with federal standards.

ARGUMENT

A. GAPS IN CYBERSECURITY COMPLIANCE

This section outlines access control deviations observed during the implementation of Executive Order 14210 and evaluates their alignment with federal cybersecurity mandates. These technical issues may assist the Court in reviewing pre-TRO agency conduct and understanding the procedural environment in place when the May 9 Order was issued. The evidence reflects delays in disabling system access after employment status changed, a core requirement for insider threat mitigation.

Records show that terminated probationary employees reported continued system access following their separation dates (see Scott Pitcock statement, Ex. A [redacted], and sealed Exhibits B–E [employee statements submitted under seal pursuant to Civil L.R. 79-5]) retained access to FDA systems after separation. My former supervisor noted that account deprovisioning tickets did not begin appearing until Tuesday, February 18, several days after terminations began and nearly three weeks before the Court's Temporary Restraining Order. These delays diverge from the following federal mandates:

- FISMA requires timely, risk based access controls.[1]
- NIST SP 800-53 mandates prompt credential termination [3] and flags delays as systemic risk. [5]
- OMB Circular A130 assigns access control responsibility to agency heads. [4]

I retained elevated administrative access to FDA infrastructure until February 18, more than 60 hours after receiving my termination notice, inconsistent with privileged access control standards.[6] As shown in Exhibit F ([redacted] emails forwarded to personal account showing retained access to FDA email), I accessed and forwarded email to my personal account during this time. My supervisor's sworn statement (see Ex E., sealed supervisor statement) confirms that system permissions remained active and deprovisioning had not begun until that Tuesday. It

documents similar delays and oversight gaps affecting another employee removed the same weekend, further underscoring the procedural uncertainty surrounding decisions during this period.

These delays reflect more than minor processing variances. They raise questions about adherence to required federal procedures and best practices, including:

- Federal identity and access management policy, including ICAM and NIST SP 800-53, requires prompt termination of system access upon separation to reduce insider threat risk. [3] [5]
- NIST SP 800-37, which, while not naming personnel transitions specifically, stresses timely adjustment of controls in response to operational change and risk exposure.[7]
- Department of Justice guidance, which indicates that unmet cybersecurity obligations may trigger enforcement under the False Claims Act.[8]
- The Civil Cyber-Fraud Initiative, which targets deficient cybersecurity practices under federal contracts, including access control failures.[9]

Access and communication patterns align with systemic deficiencies outlined in the HHS Inspector General's 2023 audit.[10] While the audit predates EO 14210, the surrounding record indicates that key vulnerabilities, particularly those involving deprovisioning delays and unclear separation procedures, remained present throughout the order's implementation.

While I recognize the sensitivity of this disclosure, being one with the access, but it is necessary to show that I and others retained privileged access without oversight. In my judgment as a former agency IT specialist, this reflected conditions consistent with high risk and high impact security lapses. The mere existence of such a vulnerability heightened insider threat exposure and disrupted basic operational norms. The operational timeline surrounding EO 14210's rollout, including a federal holiday weekend, resulted in a period during which separated employees, many under personal and professional stress, retained access without review. This

exposure was not hypothetical; it was documented, extended in duration, and introduced elevated security risk.

To better illustrate these events, the following supporting exhibits are included in the Appendix:

- Exhibit J: Post Termination Access Timeline
- Exhibit K: Timeline of Agency Action and Notice
- Exhibit L: Regulatory Requirements and Evidence of Deviation

B. TERMINATION NOTICE TIMING AND COMMUNICATION BREAKDOWNS

This section outlines the delayed, uncertified delivery of termination notices received by mail after the Court's Temporary Restraining Order, and the absence of agency follow up reported by multiple impacted employees. These circumstances may be relevant to the Court's assessment of procedural consistency during the enforcement period.

I received physical notice of termination by USPS mail on May 12, 2025, three days after this Court issued its Temporary Restraining Order (see Exhibit G1, [redacted] postmarked envelope with termination letter; see sealed Exhibit G2, [redacted] court ordered letter from a separate case with Westlaw slip and included footnote). The packet was sent using standard USPS delivery and did not require a signature. Another employee also reported receiving notice under the same conditions (see sealed Exhibit D, statement submitted to show that other employees were affected similarly). As of the date of this amicus, no corrective action has been taken as far as I'm aware.

In contrast, a prior restraining order had been communicated by email (see Exhibit H, [redacted] TRO from a different court's ruling sent to personal email on March 13, 2025). The reliance on delayed and uncertified physical mail in this instance raises concerns about procedural consistency during a period when the agency was subject to court oversight. Between

May 12 and May 22, I received no response to repeated outreach (see Exhibit I, [redacted] attempts to assert and confirm employment). No agency communication clarified my employment status beyond a leave and earnings statement (see Exhibit M, submitted in full under seal).

This lack of acknowledgment or follow-up may contribute to ambiguities in employment status, also affecting auditability under FISMA[1], which requires agencies to document control activities and maintain traceable oversight of security-relevant events. In the absence of recorded responses to post-separation inquiries, continuity and accountability may erode. This can be devastating for displaced employees when personnel actions require later verification or correction.

C. INTERACTIVE PROCESS

This section outlines communication breakdowns and the absence of an interactive process following the initial separation actions taken under Executive Order 14210. These procedural gaps are relevant to the Court's review of agency adherence to federal offboarding protocols and cybersecurity requirements. When internal communication falters during involuntary separation, it introduces ambiguity, discourages internal reporting, and increases long-term risk to security and procedural integrity.

This silence broke from standard protocol and introduced uncertainty during a period that should have followed a defined sequence of post-employment actions. My former supervisor (see sealed Exhibit E, statement and communications from direct supervisor) described leadership's reluctance to provide support, noting a sense of constraint due to direction from above. The declaration suggests that this lack of engagement affected multiple employees, indicating broader procedural breakdown.

These issues are especially significant in the cybersecurity domain. FISMA[1] and NIST Special Publication 800-53, Rev. 5 [3] emphasize the importance of reliable communication, responsive separation protocols, and documented procedures to reduce insider threat risk. When these interactive processes break down, the organization's risk profile shifts. Employees affected by opaque offboarding may lose trust, while others anticipating separation may act defensively, potentially escalating operational or security threats.

In this case, the absence of an interactive process, prolonged silence following outreach, and documented delays in deprovisioning created overlapping vulnerabilities that would be material under any standard federal cybersecurity audit. These failures reflect broader patterns documented in GAO's 2021 audit[11] of insider threat programs, which identified systemic lapses in offboarding, internal communication, and leadership responsiveness.

CONCLUSION

This brief is submitted in the interest of judicial clarity and professional responsibility. The details reflect my personal experience navigating agency procedures during the implementation of Executive Order 14210 and may assist the Court in its review of agency adherence to federal standards and this Court's directives.

Based on detailed documentation and firsthand account, the following patterns are presented for the Court's consideration:

- System access remained active after employment status changed.
- Separation communications were received after the Temporary Restraining Order.
- No formal process was communicated for initiating post-employment procedures.
- Attempts to clarify status received no documented response.

These observations are offered without attribution of fault and solely to assist the Court in assessing procedural consistency with federal cybersecurity policy and its own Temporary Restraining Order. Amicus respectfully requests:

1) The Court to consider the following: While NIST defines integrity in technical terms as protection against unauthorized modification, it also recognizes trustworthiness as a broader organizational attribute that includes integrity, transparency, and accountability. Can an agency maintain the integrity of its systems if it fails to apply those same standards to the processes that govern access, separation, and employee oversight?

2) that the Court consider the technical record, documentation, and statements provided herein as part of its evaluation.

DATED: June 6, 2025

Respectfully submitted,

/s/ Scott C Pitcock

Scott C. Pitcock (pro se)
[Address and phone number omitted from public filing in accordance with Civil L.R. 5-1(c)(5); contact information on file]
scott_pitcock@hotmail.com

ENDNOTES

1) Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (codified at 44 U.S.C. § 3551 et seq.).

2) U.S. Off. of Pers. Mgmt., Credentialing Standards Procedures for Issuing Personal Identity Verification Cards Under HSPD-12, https://www.opm.gov/suitability/suitability-executive-agent/policy/cred-standards.pdf.

3) Nat'l Inst. of Standards & Tech., Security and Privacy Controls for Information Systems and Organizations, NIST Special Pub. 800-53, rev. 5 (Sept. 2020).

4) Off. of Mgmt. & Budget, Circular A-130: Managing Information as a Strategic Resource (July 28, 2016).

5) Nat'l Inst. of Standards & Tech., Security and Privacy Controls, supra note 3, AC-2(4).

6) Nat'l Inst. of Standards & Tech., Security and Privacy Controls, supra note 3, AC-6, AC-17, CM-6.

7) Nat'l Inst. of Standards & Tech., Risk Management Framework for Information Systems and Organizations, NIST Special Pub. 800-37, rev. 2 (Dec. 2018).

8) 31 U.S.C. §§ 3729–3733 (2018).

9) U.S. Dep't of Justice, Civil Cyber-Fraud Initiative, https://www.justice.gov/civil-cyber-fraud-initiative.

10) Dep't of Health & Hum. Servs., Off. of Inspector Gen., Audit of HHS Systems Access Controls, A-18-22-11300 (July 2023).

11) U.S. Gov't Accountability Off., Insider Threats: Critical Infrastructure Entities Generally Have Controls in Place, but Could Improve Their Reporting, GAO-21-104 (Mar. 2021).

12) Nat'l Inst. of Standards & Tech., Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, NIST Special Pub. 800-137 (Sept. 2011).

APPENDIX - TABLES

Exhibit J - Post-Termination Access Timeline

Employee (Exhibit)	Termination Notice Date	Notification Received	Access Type	Access Revoked (Approx.)
S. - Ex. A	Feb 14, 2025	Feb 15, PM	Elevated + User	Feb 18, ~11:30 AM EST
F. - Ex. B	Feb 14, 2025	Feb 15, PM	Elevated + User	Feb 18, ~11:30 AM EST
G. - Ex. C	Feb 14, 2025	Feb 15, PM	User Only	Feb 18, ~11:30 AM EST
P. - Ex. D	Feb 14, 2025	Feb 15, PM	User Only	Feb 18, ~11:30 AM EST

Exhibit K - Timeline of Agency Action and Notice

Date	Event
February 14, 2025	Dated notice of initial termination action under EO 14210.
February 15, 2025	Received termination notice in the evening; reported to supervisor.
February 18, 2025	Credential revocation at approximately 11:30 AM EST.
March 13, 2025	TRO from a separate case received via personal email.
May 8, 2025	Final termination packet postmarked.
May 9, 2025	This Court's TRO goes into effect.
May 12, 2025	Received postmarked termination packet.
May 23, 2025	Final paycheck issued, including full annual leave payout.

Exhibit L - Standards and Observed Deviation

Standard / Source	Requirement	Observed Violation	Impact / Duration
FISMA – 44 U.S. Code § 3554[1]	Prevent unauthorized system access post-separation	Access remained active for >60 hrs after termination notice	High / 60+ hrs
False Claims Act – 31 U.S.C. §§ 3729–3733[8]	Prohibits knowing failure to meet obligations under federal contracts	Delayed access revocation and cybersecurity lapses risk triggering liability	High / systemic
OMB A-130[4]	Agency heads responsible for timely ICAM policy enforcement	Credential revocation lagged across terminated employees	High / 60+ hrs
OPM Credentialing Standards[2]	Terminate PIV credential access when employment ends	PIV access not confirmed revoked during 60+ hour window	Moderate / unclear
NIST 800-53 (Rev. 5)[3]	Terminate accounts promptly upon separation	Multiple users retained access 4+ days post-termination	Critical / 60+ hrs
NIST 800-53 AC-6(9), CM-6[6]	Restrict and monitor elevated access	Admin permissions retained after separation	Critical / 60+ hrs
NIST 800-63-3[12]	Revoke digital credentials	Credential access remained after employment change	High / 60+ hrs

	promptly when no longer needed		
NIST 800-37 (Rev. 2)[7]	Adjust controls after operational changes	Control changes delayed after bulk terminations	Moderate / policy-wide
DOJ Civil Cyber-Fraud Initiative[9]	Holds agencies/contractors accountable for security failures	Noncompliance with cybersecurity standards risks enforcement	High / systemic
HHS OIG Audit (2023)[10]	Document and follow separation processes	Findings mirror failures during EO 14210 implementation	High / sustained
GAO-21-104[11]	Address offboarding and communication weaknesses	Systemic parallels in delayed coordination and unclear leadership	Moderate / institutional

Table of Exhibits

Exhibit	Description	Referenced In
A	Redacted Statement of Scott C. Pitcock – Summary of termination actions and system access	Section II – Technical Facts
B	Sealed statement of Employee B – Summary of termination actions and system access	Section II – Technical Facts
C	Sealed statement of Employee G – Summary of termination actions and system access	Section II – Technical Facts
D	Sealed statement of Employee D – Summary of termination actions and system access	Section II – Technical Facts
E	Sealed declaration and communications from former supervisor – Describes offboarding delays and limited support from leadership	Sections II, IV
F	Redacted email logs showing continued access to FDA email account following Feb. 15 notice	Section II – Technical Facts

G1*	Redacted Outer envelope and postmark (standard USPS, postmarked May 8, 2025)	Section III – TRO Compliance
G2*	Redacted termination letter and Westlaw printout with disclaimer (submitted under seal)	Section III – TRO Compliance
H	Redacted copy of March 13, 2025 TRO notice from unrelated case (received via personal email)	Section III – TRO Compliance
I	Redacted emails showing attempts to confirm employment status	Section IV – Interactive Process
J	Post-termination access timeline – Documents level and duration of account access following notice	Appendix – Post-Termination Access Timeline
K	Standards and observed violations – Summary of policy requirements and procedural lapses	Appendix – Standards and Observed Deviation
L	Agency action timeline – Chronological summary of key events through final termination	Appendix – Timeline of Agency Action and Notice
M	Sealed Final Leave and Earnings Statement	N/A

*G1 and G2 were within the same envelope